NPOESS Satellite Direct-Access Data Denial

NGST – Subcontractor

npoess.noaa.gov

Advanced Encryption Standard (AES), PKI & Encryption/Decryption

The 1994 Presidential Decision Directive that created NPOESS states: “The United States will ensure its ability to selectively deny critical environmental data to an adversary during crisis or war yet ensure the use of such data by U.S. and Allied military forces.” The Integrated Program Office will implement this directive within the NPOESS program using a complement of techniques that will ensure compliance. This will assure that access to operational environmental data is provided to meet civil and national security requirements and international obligations. NOAA will be responsible for archiving all data.

All NPOESS mission data will normally be transmitted unencrypted for access by Centrals and Field Terminal Users worldwide. All users will be able to acquire the data and will not need any additional decryption capability. In the SDE Mode, NPOESS can deny data either globally or over specified regions of the world, by sensor using virtual channel IDs (VCIDs), or to individual users. Authorized, registered users will need AES (Advanced Encryption Standard) decryption capability to receive the data while in Selective Data Encryption (SDE) Mode. The Centrals however, will continue to receive the NPOESS data from each Central IDP element and control of further dissemination of the data is the responsibility of the Centrals. ADCS and SARSAT data will always be unencrypted and available even while in SDE mode.

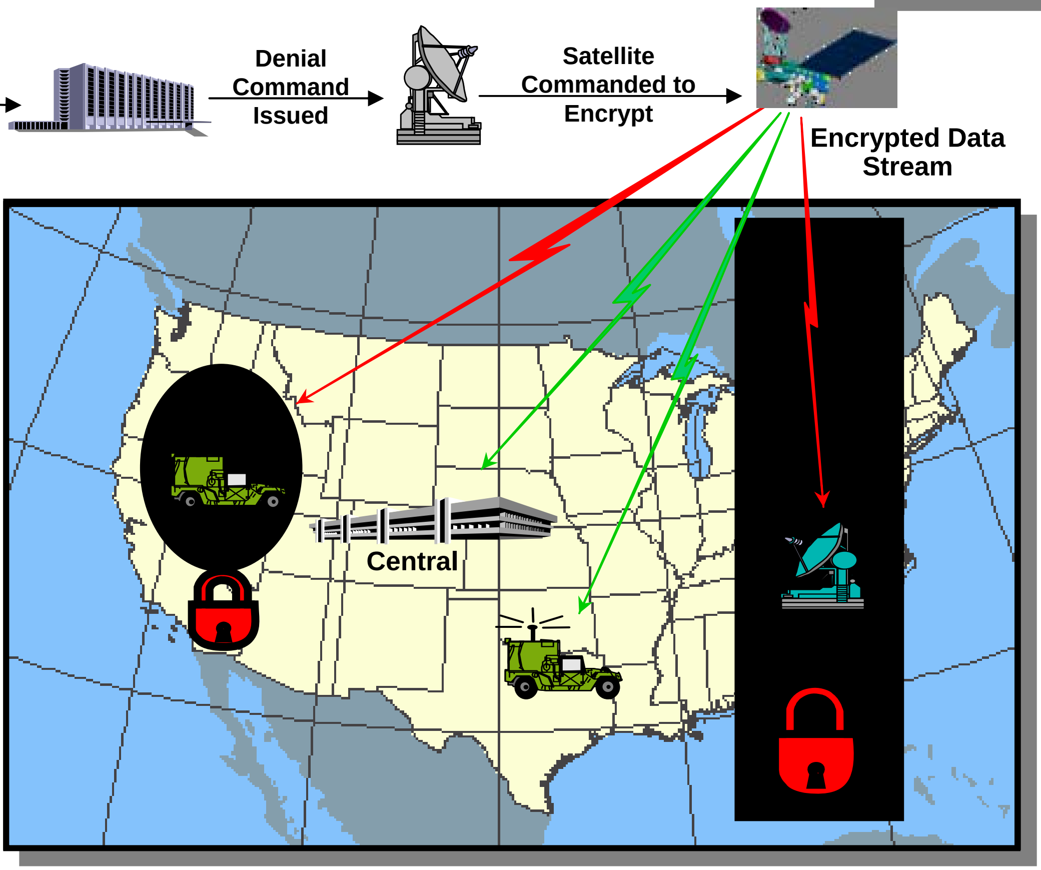
The algorithm used in AES is the Rijndael Block cipher algorithm. This is the Federal Information Processing Standard (FIPS) approved algorithm that may be used by U.S. Government organizations to protect sensitive information. NPOESS will use a 256-bit key. In decimal terms, that means there are 1.1 x 10^{77} possible 256-bit keys. This key strength has been approved by the National Security Agency for use to protect Top Secret information.

P
K
I

Public Key Infrastructure

<u>Public Key Infrastructure (PKI)</u> will be employed to ensure that confidentiality, authentication, data integrity, and non-repudiation is maintained during data denial. PKI uses asymmetric keys: encryption and decryption require different, but related keys. The public keys will be used to encrypt the data and the private keys are used to decrypt the data. More information about PKI can be found at http://csrc.nist.gov/pki

Secretary of Defense issues Data Denial Directive (DDD).



Denial Command Issued

Satellite Commanded to Encrypt

Encrypted Data Stream

Central

Key Management Plan

Users will need Fedreal Bridge Certification Authority (FBCA)-complaint PKI Public and Private Keys. The Spacecraft will encrypt the current AES Key with each users PKI public key. These key transports will be included in the downlink. The users will decrypt the AES Key using their PKI Private Key.

Regional Denial

Data in the region is denied to all users without appropriate decryption keys and decryptors, however data will be collected by the Centrals and the data will become available in accordance to national data distribution policy.

NPOESS data denial supports the operational requirements for data denial, individual receiver key enabling and revoking, and re-keying over the air. If the system transitions to SDE Mode, the authorized Registered Users will continue to process mission data. The Users that are not authorized will not be able to process mission data until the system transitions back to Normal Operations Mode. The NPOESS satellites will have the capability to encrypt the mission data in the SMD, HRD, and LRD.

Rev. 073006